UCRL-WEB-201524

Firewall and SSH Guide

Table of Contents

Preface

Scope: The Firewall and SSH Guide describes the user-relevant features of LC's security firewall that protects (some) machines in the llnl.gov domain, tells how to use indirectly the services (such as FTP) that the firewall blocks directly, and introduces alternative services (such as secure shell SSH and local variants, or Virtual Private Network VPN) intended to take the place of the blocked services. See the EZACCESS (URL: https://computing.llnl.gov/LCdocs/ezaccess) guide for a comparative general introduction to the many ways to reach LC computing resources, of which access though the firewall is only one. See the EZSTORAGE (URL: https://computing.llnl.gov/LCdocs/ezstorage) guide if you are primarily concerned about storing at LC project files that were generated elsewhere.

Availability: When the programs described here are limited by machine, those limits are included in their explanation. Otherwise, they run under any LC UNIX system.

Consultant: For help contact the LC customer service and support hotline at 925-422-4531 (open e-mail: lc-hotline@llnl.gov, SCF e-mail: lc-hotline@pop.llnl.gov).

Printing: The print file for this document can be found at:

```
OCF: http://computing.llnl.gov/LCdocs/firewall/firewall.pdf
SCF: http://www.llnl.gov/LCdocs/firewall/firewall_scf.pdf
```

Introduction

This document describes LC's security firewall. It tells how to continue using those services (such as FTP) whose normal behavior the firewall alters, and it introduces some alternative services (such as secure shell SSH) intended to take the place of the ones that the firewall blocks. See the EZACCESS (URL: https://computing.llnl.gov/LCdocs/ezaccess) basic guide for a more general, comparative introduction to the many different ways to reach LC computing resources.

Firewall Terminology

Because firewall terminology can be arcane, this introduction briefly explains some crucial terms and distinctions used later in the text. If you are already familiar with these background definitions, just skip directly to the sections about LC's specific firewall implementation and its effects on users. This document is NOT a general review of all known firewall tools and techniques, but rather practical advice for users coping with LC's particular firewall.

Data moves around computer networks in discrete packets (of bits), governed by standard rules (protocols). The well-known IP (Internet Protocol) delivers packets to intended destinations, fragmenting and reassembling messages as needed. The TCP (Transmission Control Protocol) performs error checking and handles packet retransmission if damage or loss occur. Each network "service" (such as SSH or FTP) uses a numerical extension of the receiving machine's IP address (e.g., 134.9.50.39) to keep track of packets associated with that service. This is often called a port number (e.g., 22 is the default TCP port number for SSH). Upon this basis (of protocols and port numbers) firewall security is built.

The most basic firewall technique is PACKET FILTERING. Packet filtering usually takes place at a "screening router" located on the border of a network. The screening router examines incoming packets and decides whether to block them or allow their access to different machines on the protected network by consulting a (locally supplied) list of rules. These rules can allow or block network packets based on

- packet source,
- packet destination,
- IP protocol type, or
- TCP (or other) port number.

For example, one way to prevent anyone from TELNETing to your local machines is to block packets for TCP port 23 from coming through the filter (as LC does).

A second, enhanced approach to firewall security involves PROXY SERVERS. A proxy server is software specific to each application or service (e.g., one for SSH, a different one specifically for HTTP) that aims to prevent clients outside the protected network from DIRECTLY contacting servers inside the protected network (or, sometimes, vice versa). When a firewall incorporates proxy servers, each (outside) client makes requests to the (appropriate) proxy server, which then, if allowed by its (locally supplied) list of rules, indirectly retrieves the requested information from the real server and returns it to the client.

Timeouts

Beginning in November, 2004, LLNL automatically, as a matter of policy, disconnects *every* remote-access Internet (but not OTS) session if either:

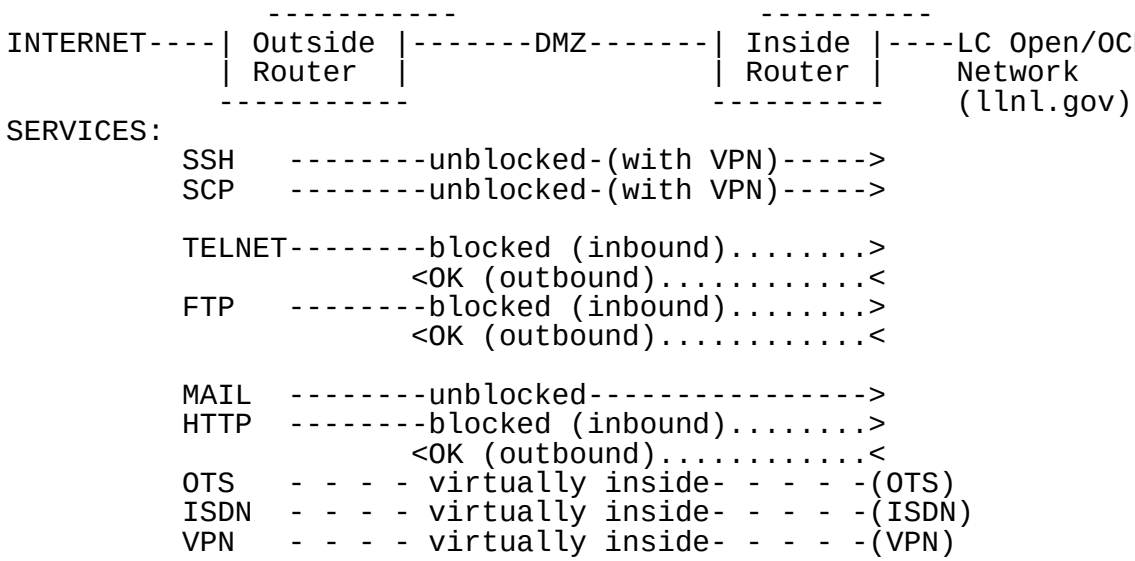
- INACTIVITY--
  the session remains inactive for more than 30 minutes or,
- ELAPSED TIME--
  12 hours elapse since you last authenticated your VPN (Virtual Private Network) session. Reconnecting with VPN resets the elapsed time.

This means that during long-running "dedicated access" production jobs, you must reauthenticate your VPN session at least every 12 hours or lose your connection to LLNL computers.

Firewall Features at LC

This section describes the design of LC's security firewall, explains how its features affect your access to LC computers, and summarizes the firewall's effect on each "service" (such as SSH) that you might use. The next section (page 9) gives detailed instructions for using each service whose behavior the firewall has changed (blocked).

This diagram shows the LC firewall and its features, and suggests its effect on each relevant service (details follow):



The LC firewall consists of these FEATURES:

Outside Screening Router

performs packet filtering on incoming network traffic (i.e., on packets coming from the Internet toward machines on LC's own open (OCF) network). Some packets (those with TELNET or FTP port numbers) are completely blocked inbound. Other packets (e.g., those with SSH or SCP port numbers) pass through unblocked. Currently, incoming MAIL packets are also unblocked. OUTWARD packets (headed from LC's network toward the Internet) or travelling among llnl.gov machines are NOT affected by this router.

DMZ ("demilitarized zone") is a subnet between two screening routers where security-enhancing software resides on "bastion hosts." Examples include
(A) GATEWAYS that demand extra authentication before allowing a service (such as SSH) to cross, or
(B) PROXY SERVERS that prevent any direct contact between clients and servers by catching and retransmitting only those packets that meet specified safety rules (for each different service).

Inside Screening Router

performs additional packet filtering on incoming network traffic. Packets with TELNET and FTP port numbers were formerly only allowed if they originated from an LC gateway within the DMZ (above), but this ended in April, 2000. SSH and SCP packets are allowed to continue from any source, as are (currently) MAIL. OUTWARD packets (headed from

LC's network toward the Internet) or travelling among llnl.gov machines are NOT affected by this router.

The SERVICES that the LC firewall manages are individually controlled to achieve different security goals. The next section (page 9) gives detailed instructions for those services whose behavior the firewall has changed. The current security "stance" toward each service is summarized here (in the order shown on the diagram above):

SSH and SCP (secure shell and secure copy) are the preferred log-on and file-transfer services that the firewall allows inward (with prior VPN (page 17)) from any source to any llnl.gov destination. SSH and SCP service outward from any supporting llnl.gov machine (and among LC machines) is also freely allowed. See the SSH (page 11) section below for advice on installation and use.

TELNET inward to any LC llnl.gov machine from any machine outside llnl.gov as well as from any nonLC llnl.gov machine (i.e., from any machine outside the 134.n.n.n IP domain) is totally blocked. (TELNET service among LC machines themselves is also blocked.) TELNET service outward from LC (134.n.n.n-domain) machines to nonLC machines is still freely allowed.

FTP inward to any LC llnl.gov machine is totally blocked. FTP service outward from (or among) llnl.gov machines is freely allowed. Running a VPN (page 17) client on your offsite computer before starting an FTP session sometimes avoids this blocking (see the FTP (page 10) section for details).

SFTP inward to any LC llnl.gov machine, including FIS, is totally blocked. Even using OTS or VPN will *not* enable SFTP access from offsite machines to FIS.

MAIL inward or outward moves freely through the firewall now (this may change later).

HTTP (World Wide Web service) has been split by locating some LLNL WWW servers outside the firewall while placing others behind it. The public servers remain available to all users (e.g., www.llnl.gov), but requests for the restricted servers are now blocked at the firewall. Running a VPN (page 17) client on your offsite computer before starting an HTTP (web-browser) session avoids this blocking.

OTS (Open Terminal Server) lies outside the LC firewall but is treated as if it were a local machine residing inside the firewall, so OTS users will see no service change. For help using the Open Terminal Server to avoid firewall problems, consult the OTS Online Manual (URL: https://access.llnl.gov/ots_access/index.html), maintained as a family of web pages by Open LabNet.

ISDN (fast telephone connection) lies outside the LC firewall but is treated as if it were a local machine residing inside the firewall, so ISDN users will see no service change.

VPN (Virtual Private Network) is a pair of servers outside the firewall (vpna.llnl.gov and vpnb.llnl.gov) that lets authorized users borrow an IP address from a domain behind the firewall so that (some) other offsite applications (such as web browsers and FTP, but not SFTP) can avoid the usual firewall service restrictions. See the VPN (page 17) section below for advice on installation and use.

Services Affected by the Firewall

This section tells how to continue using those services whose normal behavior is altered by the LC firewall (other services perform as if the firewall did not exist).

TELNET (Obsolete)

LC requires offsite users to run secure shell SSH (page 11) instead of TELNET to log on to open-network LC machines. For this reason, LC's firewall allows SSH traffic from any outside host but totally blocks all TELNET traffic from every host outside the 134.n.n.n IP domain (that is, blocks all TELNET traffic from all non-LC hosts, including llnl.gov hosts outside the LC-controlled 134 IP domain). Similarly, TELNET traffic among LC machines themselves is blocked. Only client TELNET service outward from 134.n.n.n machines to other IP domains remains. See the SSH (page 11) section below for the best current alternative.

FTP

LC's firewall totally blocks all FTP traffic from every host outside the llnl.gov domain. To transfer files from machines outside llnl.gov to any LC machine, outside users have two choices:
(1) Log on to an LC machine first, then execute FTP on that machine and connect back to the outside machine where the sought files reside, using GET to retrieve them. It also requires that an FTP server (not just a client) run on the outside machine, a problem for some workstations.
(2) Run a VPN (Virtual Private Network) client on your outside machine before you start your FTP file-transfer session. VPN temporarily borrows an llnl.gov IP address for the machine where it runs, thus enabling other programs (such as FTP) to act as if they were running inside, not outside, the firewall. You must first get a VPN account, download the VPN client appropriate for your operating system, and configure it for use with LLNL's VPN server (instructions are in the VPN (page 17) section below).

FTP USAGE WARNINGS:

Storing Files.
LC's open file-storage system (HPSS) does NOT accept secure copy SCP connections. So offsite users who want to store files archivally in HPSS must either
(A) log on to some llnl.gov LC machine using SSH, execute FTP there and GET their remote files, then PUT those files from the LC machine into storage.llnl.gov, or
(B) use SCP (under VPN) to move their files to some llnl.gov LC machine, and then use SSH to log on to that machine and execute FTP there to secondarily move the files again to storage.llnl.gov.

Secure FTP (SFTP).
SFTP connections (to FIS) work only from OCF machines within LC's firewall. Even using OTS or VPN will *not* enable you to connect from an offsite machine by running SFTP.

Secure Shell (SSH)

Role of SSH

The secure shell (SSH) is a product (for which there are public domain and licensed versions) designed to provide an easy, secure connection (over an unsecure channel) between two Internet sites. SSH, once installed and initialized on both the local and remote machines, allows you to

- log in to the remote computer,
- execute commands on the remote computer,
- move files between the local and remote machines (using SCP), and
- provide secure X connections.

SSH is intended to replace the less secure programs RLOGIN, RSH, and RCP, and it mostly shares their syntax. SSH has two prime security advantages over RSH and TELNET for between-machine connections:

- The data and control stream between SSH sites are enciphered to deter network packet sniffing. File transfers using SCP are fully enciphered too, but if you use FTP to "tunnel through" an SSH session to transfer files, only the control stream is encrypted, not the date stream.
- Strong authentication of both hosts and users is performed using robust "public-key" cryptography. No clear-text passwords are sent.

At LC, SSH packets pass unblocked through the firewall in both directions, while RSH has been discontinued and TELNET service is blocked both from outside inward to, and internally among, all LC llnl.gov machines.

Currently, LC only supports the SSH version 2 protocol.

Setup of SSH (and Troubleshooting)

SSH requires several careful, preliminary setup steps, and you must repeat these steps for every pair of (local and remote) machines between which you want to use SSH connections.

Basic Software Installation

In the unclassified environment (at LC or on any Internet site), to use SSH properly and to gain all the security advantages it offers (see above), you should run SSH on the machine on your desktop. If you use an X terminal, SSH should be installed on the machine that supports your terminal sessions.

For help obtaining, installing, and configuring SSH clients on Macintosh computers, UNIX systems, or Windows machines, please contact your local computer systems support staff.

Until SSH is installed on your local machine you can still gain some security benefits by using SSH between LC hosts. The next two sections (below) apply to UNIX machines whether you are using SSH from your desktop or from one LC host to another. The "local" machine is always the one where you execute SSH; the remote or target machine is the system to which you want to connect using SSH.

Local Host Initialization

In most cases, your local desktop machine should already have the lab-approved SSH software installed on it. Support for desktop software is handled through the institutional 4HELP hotline: x4-4357 (phone), 4hlelp@llnl.gov (e-mail) or 4help.llnl.gov (web). LC has prepared setup and configuration instructions for Windows machines, please see Configuring the Reflection SSH Client and X-Win32 for Connection to LC Machines (URL: https://computing.llnl.gov/?set=access&page=reflection_ssh_setup).

LC Host Initialization

The following steps describe how to set up RSA/DSA key authentication:

(1) Execute **`ssh-keygen -t type`** where type is either "rsa" or "dsa" — Take your pick

(2) When prompted enter a passphrase if you want improved security. If you want the convenience of being able to ssh into other LC OpenSSH machines without entering a userid/password, don't enter anything.

(3) After the command completes, **`cd`** to your **`.ssh`** file and copy the file which ends in **`.pub`** to a file named **`authorized_keys`**. This is your public key. For example:

```
cp id_dsa.pub authorized_keys
```

(4) Because all OCF/SCF machines share the same home directory, you don't need to copy your public key file to each host. One copy does the trick.

(5) Make sure than your .ssh files are readable only by you.

Troubleshooting SSH

Here are some common SSH problems and the suggested responses to them:

- NO DAEMON.
  You cannot use SSH to contact any host that is not already running the SSH daemon. Contact the host's system administrator (or the LC Hotline) if you think the daemon has not been installed.
- WRONG PERMISSIONS.
  Check that your target home directory does not allow world or group WRITE access; such access causes SSH to fail. (For example, 700 and 755 are compatible with using SSH, but 766 is not.) Use CHMOD to reset the faulty permissions.
- AUTHORIZATION FILE FLAWS.
  Check that the IDENTITY.PUB line was appended to the target host's AUTHORIZED_KEYS file as a single long line with no breaks. Careless editing can insert returns into this line, spoiling it.
- HOST KEY QUERY 1.
  If you attempt to connect to a target host using SSH and receive the message

  ```
  Host key not found from the list of known hosts.
  Are you sure you want to continue connecting (yes/no)?
  ```

  simply respond YES (warning: typing Y alone will be inadequate). SSH will update its list of known hosts (where it regards ATLAS and ATLAS.LLNL.GOV as different machines).
- HOST KEY QUERY 2.
  If you attempt to connect to a target host using SSH and receive the message

  ```
  @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
  @       WARNING: HOST IDENTIFICATION HAS CHANGED!       @
  @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
  IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
  Someone could be eavesdropping on you right now
  (man-in-the-middle attack)!
  Are you sure you want to continue connecting (yes/no)?
  ```

  simply respond YES and SSH will add another entry to your local ~/.ssh/known_hosts file. This message usually occurs because SSH considers ATLAS and ATLAS.LLNL.GOV to be different machines, for example, despite your earlier successful setup work on a target host.
- OTHER PROBLEMS (VERBOSE MODE).
  You can always run SSH with the -v (verbose) option to gather additional troubleshooting clues. Or run the KLIST utility to report on the current status (expiration date, etc.) of your "kerberos authentication ticket."

Using SSH (UNIX)

Whenever you use an SSH client on an outside-the-firewall (outside llnl.gov) machine to connect to an LC OCF machine, remember to:
(1) Authenticate with VPN (page 17) before you execute SSH (except LANL/Sandia), or
(2) Use port 922 (-p 922) (via LANL/Sandia)

When you log on to a (UNIX) machine using SSH, your customization (dot) files are executed and you arrive in your home directory. Your path and other environment variables are set by your dot files. If you do not specify a full pathname for a remote command, the value of $PATH is used for the search path. The default current location (invoked in a syntax such as ./myscript) is your home directory.

WARNING: When you execute a command remotely using SSH *without* logging in to the remote host, however, SSH usually does *not* execute the command in a login shell. Usually, your customization (.login, .profile) files are *not* executed, so your environment variables (including PATH) are not set as they would be if you had logged in. This may cause your remote command to fail or misbehave.

Here are some typical SSH execute lines, with explanatory comments shown in their most general form. Note that LANL and Sandia users coming from their unclassified internal networks must also supply the **`-p 922`** option with their ssh commands.

- Simple log on:

```
ssh targethost
example: ssh atlas.llnl.gov
```

  (makes the current window a session on ILX1).

- Log on with different target user name:

```
ssh -l LCusername targethost
example: ssh -l arn atlas.llnl.gov
```

  (local user arnold with LC username arn logs on to ILX1).

- Execute command on target host:

```
ssh targethost targetcommand
example: ssh atlas.llnl.gov xterm
example: ssh atlas.llnl.gov ./myscript
```

  (runs the specified command as if you had logged on).

- Execute command on target host with different username:

```
ssh -l LCusername targethost targetcommand
example: ssh -l arn atlas.llnl.gov xterm
example: ssh -l arn atlas.llnl.gov ./myscript
```

  (runs the specified command as if you had logged on as arn).

An alternative overview of contacting LC computers from outside the llnl.gov domain by using SSH (including some additional, varied examples) is available on the Access Information page (URL: https://computing.llnl.gov/?set=access&page=index#logging-in1).

Virtual Private Network (VPN)

Virtual Private Network (VPN) is a way to temporarily borrow an llnl.gov IP address (from a pool for that purpose), so that while a VPN client runs on your outside-the-firewall machine all other applications there (such as your web browser or your FTP client, but not SFTP) perform with the same privileges that they would have if your computer were inside instead of outside the LLNL firewall.

VPN use requires that you download and install a VPN client on your machine and then execute it during every VPN authenticated session, or you can use the Web-based SSL VPN client. Your VPN client interacts with a corresponding VPN server at LLNL while it runs. VPN clients for Macintosh (OS X), Windows (XP or 2000 only), and UNIX (Solaris or Linux) platforms are available to authorized LC users for free download from the LLNL VPN Access page (URL: https://access.llnl.gov/vpn_access), as noted in the next subsection. Only LLNL employees (or contractors) and certain other ASC collaborators can establish an authorized VPN account, whose ID and password (now the same as your LC authenticator-generated one-time password) are required to run the VPN client, by contacting the LC Hotline (paperwork and approvals are required).

The subsections below tell how to get an appropriate VPN client for your outside-the-firewall machine, how to install and configure it, and how to run it to enable VPN-authorized use of your other programs.

Getting a VPN Client

VPN client executable files for Macintosh (OS X), Windows (XP or 2000 only), and UNIX platforms (Solaris and Linux) are available to authorized users for free download from the LLNL VPN Access page (URL: https://access.llnl.gov/vpn_access).

Offsite users must already have an authorized VPN account so that they can provide their official VPN ID (not LC login name) and VPN password before the download begins (contact the LC Hotline to get an account). Onsite users will not be asked for authentication to download clients. The client files are only about 1 Mbyte, so if downloading directly to your offsite machine poses a problem, you could download the appropriate client to an LC machine and e-mail it to yourself as an attachment.

VPN users who had already installed the VPN 5000 client before October, 2005, will need to uninstall it first, and then install the newer VPN 3000 client (currently available on the above web site). Only VPN 3000 will be supported by LLNL's VPN servers in the future.

Installing and Configuring VPN

INSTALL.
To install your downloaded VPN client in either the Macintosh or Windows environment, just double click on the downloaded executable file. This starts an installation wizard that leads you through several screens of set-up steps. After installation, the wizard offers to restart your computer, which is necessary to make VPN available for use.

CONFIGURE.
To configure the VPN client once installed, follow the links called "Setting Up the VPN 3000 Client" that appear in the middle of the LLNL VPN Access page (URL: https://access.llnl.gov/vpn_access).

If you had already installed the VPN 5000 client before October, 2005, then you will need to uninstall it first, then install the newer VPN 3000 client to take its place.

Using VPN to Contact LLNL

Your local VPN client interacts with a VPN server at LLNL while it runs. So sometimes (unacknowledged) problems with the server will prevent you from successfully starting a VPN session. This is usually self-correcting, so just try again if your request for a connection is at first refused.

To use your VPN client (after installing and configuring it, above), follow the links to "LLNL VPN 3000 Client Documentation" or "Cisco VPN 3000 Client Documentation" that appear in the middle of the client-distribution Web page at the LLNL VPN Access page (URL: https://access.llnl.gov/vpn_access).

After your VPN client confirms your connection to LLNL, leave it running throughout your session so that your borrowed llnl.gov IP address remains available to other programs. You can now run other applications (such as a web browser to access LLNL-only web sites) as you normally would. All should behave as if your outside-the-firewall machine were within the llnl.gov domain (although web traffic to other, nonLLNL sites goes and comes directly to those sites, not by way of LLNL).

Three warnings apply:
(1) If your web browser is configured to use a proxy server, then you must reconfigure it to NOT use a proxy server (just the reverse of the setting required for Web Proxy Service).
(2) If you are connecting back from LLNL (using X-windows, for example), then you must use the name that VPN temporarily assigns to your computer (of the form vpn###.llnl.gov). On the VPN client window, click on the LOGGING tab (along the top) to see a screen that reveals the current name or IP address (depends on client) assigned to your computer for this session.
(3) LC has confirmed that VPN enables inward file transfers with FTP (even to storage) when FTP and VPN run under Windows, but you may encounter vendor-compatibility problems with other operating systems.

SSL VPN Services

This service provides secure access to internal LLNL resources much like the IPsec VPN service. In many cases, SSL VPN is easier to configure and use since the client software can deployed through a web browser interface.

For more information, see the LLNL SSL VPN Web site (URL: https://access.llnl.gov/sslvpn_access/).

Disclaimer

Keyword Index

To see an alphabetical list of keywords for this document, consult the next section (page 22).

Keyword	Description
scope	Topics covered in this document.
availability	Where these programs run.
who	Who to contact for assistance.
introduction	Background terms and distinctions.
terminology	Firewall vocabulary explained.
timeouts	LLNL mandatory remote-access timeouts.
firewall-features	Diagram and analysis of LC firewall.
services	Instructions for firewall-altered services.
telnet	TELNET blocked inbound; alternatives.
ftp	FTP blocked inbound; alternatives.
ssh	Secure shell (SSH) instructions.
ssh-role	What SSH does.
ssh-setup	How to set up SSH.
installation	SSH installation advice (UNIX).
lc-host-init	Initializing SSH on an LC host.
local-init	Initializing SSH on a local host.
troubleshooting	Common SSH problems addressed.
ssh-execute-line	Typical SSH execute lines.
vpn	Virtual Private Network instructions.
vpn-client	How to get a VPN client.
vpn-config	How to install, configure VPN client.
vpn-ssl	Information about the LLNL SSL VPN Service.
vpn-usage	How to routinely use VPN connections.
index	The structural index of keywords.
a	The alphabetical index of keywords.
date	The latest changes to this document.
revisions	The complete revision history.

Alphabetical List of Keywords

Keyword	Description
a	The alphabetical index of keywords.
availability	Where these programs run.
date	The latest changes to this document.
entire	This entire document.
firewall-features	Diagram and analysis of LC firewall.
ftp	FTP blocked inbound; alternatives.
index	The structural index of keywords.
installation	SSH installation advice (UNIX).
introduction	Background terms and distinctions.
lc-host-init	Initializing SSH on an LC host.
local-init	Initializing SSH on a local host.
revisions	The complete revision history.
scope	Topics covered in this document.
services	Instructions for firewall-altered services.
ssh	Secure shell (SSH) instructions.
ssh-execute-line	Typical SSH execute lines.
ssh-role	What SSH does.
ssh-setup	How to set up SSH.
telnet	TELNET blocked inbound; alternatives.
terminology	Firewall vocabulary explained.
timeouts	LLNL mandatory remote-access timeouts.
title	The name of this document.
troubleshooting	Common SSH problems addressed.
vpn	Virtual Private Network instructions.
vpn-client	How to get a VPN client.
vpn-config	How to install, configure VPN client.
vpn-ssl	Information about the LLNL SSL VPN Service.
vpn-usage	How to routinely use VPN connections.
who	Who to contact for assistance.

Date and Revisions

Revision Date	Keyword Affected	Description of Change
20May09	vpn-ssl	VPN SSL Details
03Sep08	cryptocard	section deleted
	ssh-role	deleted historical information
	ssh-macintosh	section deleted
	ssh-x11-forwarding	section deleted
	ssh2	section deleted
	ssh-ipa	section deleted
	xssh	section deleted
17Sep07	terminology	TELNET details, former machines deleted.
	telnet	Comparisons useful, software obsolete.
	troubleshooting	Examples updated.
09May06	ssh-x11-forwarding	New section on Mac X11 forwarding.
	index	New keyword for new section.
04Jan06	vpn	Details replaced with new cross refs.
19Oct05	timeouts	VPN 12-hour timeout noted.
	firewall-features	IPA now very rare.
	ftp	IPA alternative deleted.
	ssh-ipa	IPA now only for rare non-VPN users.
	vpn	URL and VPN servers changed. VPN 3000 replaces VPN 5000.
12Sep05	ssh-role	Only SSH version-2 procotol supported now.
	installation	Only SSH version-2 protocol supported now.
	ssh2	OpenSSH vs SSH2 differences clarified.
22Jun05	timeouts	IPA timeout now only 2 hours.
	ssh-ipa	IPA timeout now only 2 hours.
	ssh-role	IPA timeout now only 2 hours.
16May05	terminology	New subsection created.
	timeouts	New section added.
	index	New keywords for new sections.
	firewall-features	Cross ref added to online OTS manual.
	ssh-ipa	Cross ref on timeouts added.
	ssh-execute-line	Cross ref to other examples added.
15Sep03	xssh	New section, local alternative.
	ssh-role	Cross ref to XSSH added.
	ssh-execute-line	Environment variable warning added.
	index	New keyword for new section.
01Apr03	vpn	Primary, secondary servers explained.

	ssh-ipa	IPA now uses OTP.
	firewall-features	Two VPN servers noted.
12Feb03	firewall-features	SFTP service added.
	ftp	Comparison with SFTP added.
	ssh2	DSA authentication for SFTP ok.
	ssh-execute-line	ILX replaces LX in all examples.
25Mar02	scope	Cross ref. added for EZSTORAGE.
	ftp	Former machines no longer exist.
10Dec01	ssh2	New section on SSH2 and DSA.
	ssh-setup	RSA aspects clarified.
	ssh-execute-line	When to use -p 922 clarified.
	index	New keyword for new section.
08Oct01	ftp	Anonymous FTP at ftp.llnl.gov only.
	ssh-role	SSH now OTP enabled (OCF).
	ssh-ipa	IPA password is not OTP.
	vpn	VPN password is not OTP.
09Apr01	vpn	New section explains VPN role, use.
	ssh-ipa	New section on IPA authentication of SSH.
	firewall-features	VPN added, SSH changed for IPA.
	ftp	VPN enables FTP through firewall.
	ssh	Technical updates (port 922, IPA).
	index	New keywords for new sections.
06Feb01	firewall-features	TELNET among LC hosts blocked.
	telnet	TELNET among LC hosts blocked.
	ftp	Annonymous FTP clarified.
	ssh-role	More TELNET blocking noted.
10Apr00	entire	Gateway, CRYPTOCards disabled.
		All sections revised.
25May99	firewall-features	TELNET blocking scope expanded.
	telnet	TELNET blocking scope expanded.
10May99	ssh-role	Data encryption clarified.
	ssh-setup	UNIX aspects clarified.
	ssh-macintosh	New Mac instructions added.
	index	New keyword added.
23Feb99	ftp	Firewall blocking enabled.
	firewall-features	FTP blocking enabled.
	ssh-setup	Another SSH source added.
25Jan99	entire	First edition of Firewall/SSH manual.

ANG (20May09)

UCRL-WEB-201524

LLNL Privacy and Legal Notice (URL: http://www.llnl.gov/disclaimer.html)

TRG (17Sep07) Contact on the OCF: lc-hotline@llnl.gov, on the SCF: lc-hotline@pop.llnl.gov